证券行业网站业务系统 IPv6 网络安全风险及防护技术探索

（上证所信息网络有限公司所供稿）

摘要：随着 IPv4 网络地址的消耗殆尽，互联网技术的发展需要新一代的互联网协议的支撑。近年来证券期货行业 IPv6 网络建设快速发展，核心机构、会员单位围绕网站业务系统的 IPv6 部署、IPv6 应用资源建设、双栈协议转换等方面开展了一系列工作。IPv6 网络下的安全问题也成为了一个亟需解决的热点问题。本文分析了广泛使用 IPv6 协议所面临的风险挑战，并探索实践了有效的安全防护策略。

关键词：网络安全、IPv6、安全防护

一、概述

随着移动互联网、物联网、工业 4.0 等新兴产业迅速发展，现今互联网协议第四版（IPv4）已远远不能满足万物互联、人工智能的发展需求了，而下一代互联网协议（IPv6）拥有 128 位的地址长度,广阔的网络地址空间甚至可以为地球上每一粒沙子分配一个 IP 地址，完全满足发展需要。且其网络数据报文基本由 40 个字节（Byte）的报头与扩展报头组成，相较于 IPv4 的报文结构更加简单。经过多年的发展，目前证券期货行业的 IPv6 的覆盖面已非常广泛，其技术应

用完全成熟，已经成为行业中网站业务系统的通用基础，IPv6 技术本身具备较高的机密性和完整性。

二、证券行业网站业务 IPv6 发展现状

2019 年 1 月,中国人民银行发布关于金融行业贯彻《推进互联网协议第六版(IPv6)规模部署行动计划》的实施意见（后文简称《实施意见》），对金融行业推进 IPv6 规模部署的原则、目的、范围、进度提出具体的要求，以渐进式推进与增量式推进相结合的方式，完成面向公众服务的、支持 IPv6 连接访问的互联网应用系统的建设升级。在国家政策的推动下，学习银行和保险等成熟的 IPv6 治理方案，证券期货行业加速推进 IPv6 的部署规模。

当前行业内各核心机构已基本完成 IPv6 部署，全面支持 IPv4 和 IPv6 网络运行。办公部分区域试点部署了纯 IPv6 网络环境，全面支持 IPv6 用户终端接入，同时各机构的门户网站和重要互联网信息系统均支持 IPv6 访问。但在当前的网络环境中，IPv6 协议并不能立即取代 IPv4 协议[1]，在未来很长一段时间中，二者将共存在同一网络环境中。在这段过渡时期，主要有三种技术可用于二者的兼容：一是双协议栈技术,通过保有一个 IPv4 协议栈以及一个 IPv6 协议栈，实现并轨运行；二是隧道技术，将局部 IPv6 网络的 IPv6 数据包作为数据封装到 IPv4 数据包，使得 IPv6 数据包可以在 IPv4 网络中传输；三是网络地址转换（Network Address Translator，NAT）技术，通过 NAT 实现 IPv4 和 IPv6 主机的互通。

三、IPv6 网络面临的安全风险

随着 IPv6 技术快速普及和大规模的使用，给证券期货行业的网络安全工作带来了新的挑战，具体表现以下几个方面：

1.1 过渡方案的安全风险

目前各机构的 IPv4/IPv6 处于共存时期，不论是采用双栈、隧道、还是网络地址转换，都会引发新的安全挑战。在双栈环境下，各机构普遍运行情况同时并行着 IPv4/IPv6 两个逻辑通道，因为其中一个协议的漏洞引发的攻击，可能会通过支持双栈的网络节点，在逻辑上的两张网络中相互传播，进而影响整个网站业务系统核心网和办公网的正常运行。如图 1 所示，攻击者可利用 IPv6 协议栈漏洞，针对双栈网关发起 DDoS 攻击，导致 IPv4、IPv6 网络均受影响。此外，双栈意味着网站业务系统核心网络出口、数据中心防火墙、流控等防护设备要配置双栈策略，网络管理更加复杂，被攻击的概率也会相应增加[2]。

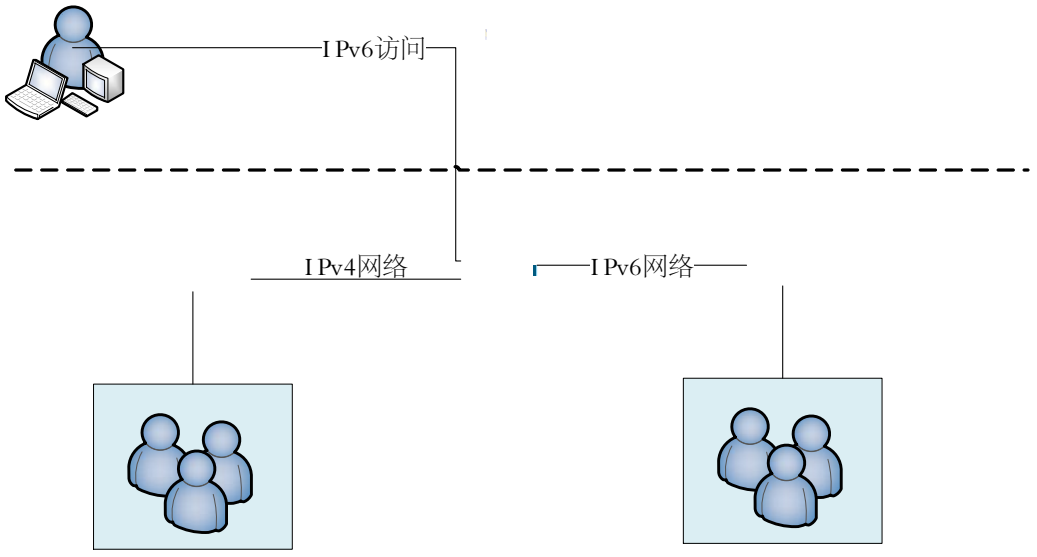

图 1 双栈环境风险

通过网络地址转换（NAT64/IVI）实现 IPv4 与 IPv6 网络的互通，也会面临常见的 DDoS 攻击的风险。如图 2 所示，通过伪造大量 IPv6 地址发起地址转换请求，攻击将导致映射 IPv4 地址池快速被消耗，转换节点无法为网站业务的正常访问用户分配转换地址，进而影响网站对外的服务。

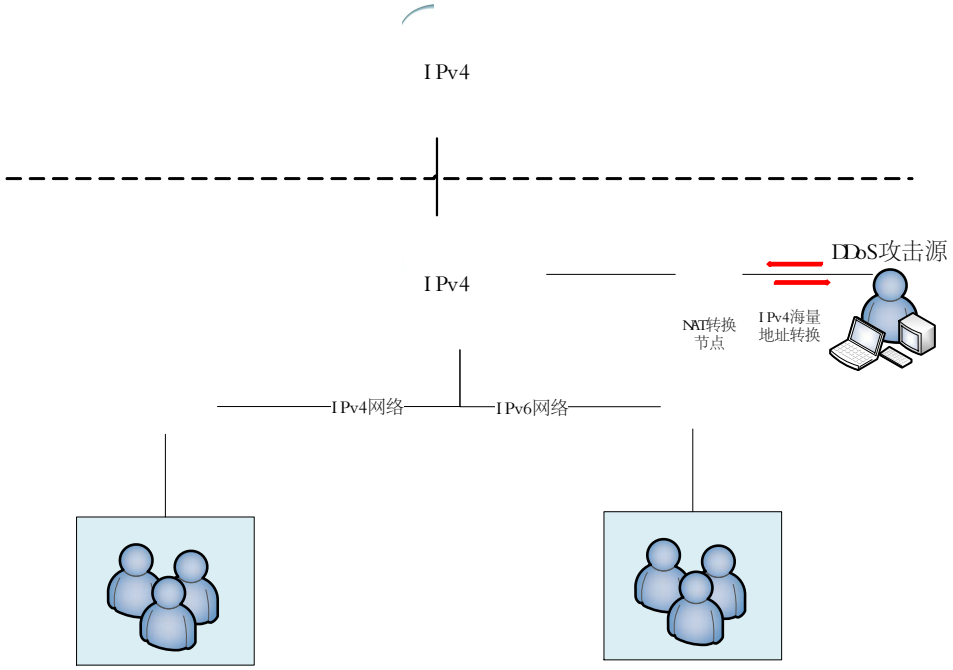

图 2 NAT 环境风险

1.2 地址资源池隐私风险

面对庞大的 IPv6 地址资源，任何物理节点都可以轻松获得 Internet IP 地址，从而促进点对点访问。如果所有网络设备都可以通过互联网访问，那设备上的个人用户就很容易通过网络被追踪。这个问题很早就被弗吉尼亚理工大学的研究团队发现了，在前期的一份报告中分析道：如果标准系统接收到 IPv6 地址，在自动配置地址（DHCP）的情况下，第三方将可以通过简单的指令（诸如 ping、traceroute 等）

在全球范围追踪和监视目标用户。同时用户发送数据的接受方信息，也会被第三方监视者获取[3]。

1.3 网络安全运维风险

一方面由于IPv6网络协议自身的限制[4]，其不能严格禁止分片组装的特点，导致网络攻击者可以绕过防火墙。分片方式的差异，使得IPS需要重新组装报文，会不在其检查和审核范围内。IPv6不能像IPv4一样随意丢弃报文中的字节，所以存在一定的安全隐患。另一方面IPv6发展对应着带宽时代发展，网络攻击成本相对较低，攻击容量较大，也便于获取，对网络安全架构设计得要求具有较大挑战。

1.4 管理安全风险

由于IPv6的地址数量众多，使得对于地址的统一分配和管理较为困难，证券期货行业内部对于地址的分配和管理尚未形成有效的管理规范。另外由于IPv6网络协议需要使用公私钥进行身份的认证，目前国内各行业对于加密算法的要求和规范未形成最佳实践和标准规范。同时，各机构忙于IPv6在使用和部署方面的技术问题,而忽视了相关网络安全知识的培训,部分终端使用者的网络安全意识缺乏,为IPv6网络的使用埋下了安全隐患。

四、IPv6网络安全风险的防护策略

1.1 系统保障过渡阶段

结合各机构过渡阶段的方案，网络安全设备需同步支持纯IPv6环境下、过渡期间IPv4/IPv6 双栈、NAT转换及隧道等场景,充分考虑IPv4和IPv6两个逻辑通道的安全需求。

日常网站业务所部署的网络环境中，防火墙设备需要支持IPv4/IPv6双栈协议及过渡时期的常用隧道技术，同时其应用网关要支持IPv6解析，病毒检测、入侵防御（IPS）等功能所需的规则库均需要升级，以支持IPv6或IPv4/IPv6双栈场景。系统思维前提下，在日常运维中需要对各设备配置的IPv4/IPv6安全策略进行一致性校验。

1.2 注重隐私泄露防范

一方面，网络安全设备采用Privacy Enhancing Technologies（隐私增强技术，PET）也对IPv6网络下的安全防护起到了重要作用。在启动IP协议头之后，可通过添加新的扩展协议头轻松扩展IPv6。在网络层，隐藏客户端的MAC地址，IP消息中的MAC地址可以采取部分加密机制。在应用层，操作系统的隐私技术可以对新操作系统中的机器隐藏某些MAC地址。另一方面，弗吉尼亚理工大学的研究团队发现采用Moving Target IPv6 Defense (MT6D)实现动态变化地址可以保护机构用户的隐私，使得通信双方实现匿名和安全的通信。MT6D类似于跳频技术，当两台主机在IPv6网络中通信时，攻击者拦截到的是多个独立主机地址的配对，无法判别哪个地址配对才是真正的通信双方，继而无法简单的对某个地址进行攻击。

1.3 强化网络安全管理

基于IPv6流量展开多样化的安全监测，科学的应用真实源地址验证技术，提升整体网络安全威胁感知能力。对各网络安全设备进行升级改造，使得其能全面满足IPv6网络

下的安全防护要求，同时加快推进软硬件系统以及相关应用系统能全面升级改造，做好网站业务系统和网络运行状态的集中监控。

1.4 动态完善管理策略

在今后 IPv6 带宽需求井喷式发展中，一是在基础环境建设规划中提前考量网络安全设备选型与网络部署，预留充足的网络性能提升空间。二是，技术人员要动态的加强 IPv6 网络安全体系的研究分析和应用，全面落实国密、商密的要求形成行业密码算法的最佳实践和行业标准。三是，技术人员要参与到专业化安全培训中，掌握更多 IPv6 知识，提升网络安全意识。同时在强化网络安全宣传基础上，普及更多 IPv6 知识，提高网络安全教育成效。

五、结语

随着 IPv6 在证券行业网站业务系统群的全面推广应用，各机构应始终遵循安全先行的原则，结合过渡阶段的网络与系统的建设需求，梳理 IPv6 带来的安全风险，尽可能地在网站业务系统立项、设计和日常的管理中完善 IPv6 安全防护。学习 IPv4 网络下安全态势感知和业务安全运行的保障能力，收集和发布 IPv6 攻击态势、IPv6 攻击分布、IPv6 威胁预警等威胁情报数据，着力提升证券期货的 IPv6 主动防御水平。

参考文献

[1] 高秋燕. 基于高校的 IPv6 网络安全研究与实现 [J] .信息系统工程， 2021, (2): 55-56.

[2] 朱慧. 高校 IPv6 网络安全风险及其应对策略研究[J] . 网络安全技术与应用, 2021, (07)： 98-100.

[3] 张连成，郭毅. IPv6 网络安全威胁分析[J]. 信息通信技术，2019，13(06)：7-14.

[4] 戴仁杰. IPv6 环境下的网络安全风险及防御措施[J]. 中国高新科技，2020(15)：143-144.

[5] 黄锐，居宏伟. 推进 IPv6 规模部署 保障金融网络安全[J].金融电子化,2020(02):20-21.